BY ORDER OF THE CHIEF,
NATIONAL GUARD BUREAU

AIR NATIONAL GUARD
INSTRUCTION 36-8001

28 MAY 2004

Personnel

AIR NATIONAL GUARD TRADITIONAL GUARD MEMBER TELECOMMUTING POLICY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: ANG/DPFS (Major A. Jackson)

Certified by: NGB/CF (Col D. Larrabee)
Pages: 12
Distribution: F

This instruction establishes the policy and guidelines for the use of telecommuting by Air National Guard (ANG) personnel. It complies with standards set forth by the following memorandums, public law and regulations: White House memorandum, 11 July 1994, Family-Friendly Work Arrangements in the Executive Branch; Deputy Secretary of Defense memorandum, 3 March 1995, Expanding Flexible Work Arrangements in the Department of Defense; Under Secretary of Defense memorandum, 20 May 1996, Department of Defense Telecommuting Pilot Project; Public Law 104-52, Page 109 STAT.468, Section 620; 31 United States Code (USC) Section 1348 /01/16/97; AFI 33-111, *Telephone Systems Management*; AFI 33-112, *Computer System Management*; AFI 33-202, Network and Computer Security *Force Computer Security Program,* AFPD 33-2, *Information Protection*; ANGI 33-103, *Internet and Electronic Mail Policy*; AFPD 36-80, *Reserve Training and Education*; ANGI 36-2001, *Management of Training and Operational Support within the Air National Guard.* States are encouraged to supplement this instruction to meet local needs. This publication is only applicable to Traditional Guardsmen.

Section A—General Information

1. Background.

1.1. Telecommuting is a management tool that allows the ANG to authorize personnel to voluntarily work away from their official duty location. Telecommuting is a complementary way of doing business, which moves work to the people instead of moving the people to the work. In general, it means working from an alternate work location away from the official duty location. Traditional telecommuters have used dial-up laptops, telephones and facsimiles to provide office communications away from the office. Virtual private networking and high-speed internet access have enhanced both electronic security and capability for telecommuters. This instruction establishes, sets forth and governs commanders' authority with respect to the types of training and duty that may be performed by all telecommuters of the ANG in accordance with Federal statutes and Department of Defense (DoD) policy. This instruction does not limit any type of training or operational support provided by member

(hereafter referred to as telecommuter) of the ANG as may be permitted without regard to this instruction.

1.2. Telecommuting is voluntary. The approval authority should grant telecommuting only when it is in the best interest of the ANG. Telecommuting is a privilege and not a right for the telecommuter. Travel in connection with this type of duty is not authorized.

1.3. This instruction requires that participants use a pre-authorized work agreement for accountability. **Attachment 2** shows a sample work agreement.

2. Scope. Telecommuting, as a management tool, authorizes commanders (or their written designees) to allow ANG drill status Guard members to work in an official capacity for pay and/or points away from the official duty location. The alternate work locations must have the necessary tools and environment to enable the telecommuter to accomplish assigned duties. All data, documents or products developed are the sole property of the United States Government and will be prepared for filing in accordance with command guidance if it is to be a permanent record. *No classified material will be used or created while telecommuting*. The approval authority and the supervisor determine the percentage of telecommuting work. Under no circumstances should a telecommuter perform all of their duties by telecommuting.

3. Roles and Responsibilities.

3.1. The Headquarters/Wing/Group/Geographically Separated Unit Commander (or their written designee) is the approval authority for telecommuting and work agreements.

3.2. The immediate supervisor is responsible for:

3.2.1. Recommending the telecommuting project to the approval authority.

3.2.2. Preparing required documents and obtaining any necessary signatures (**Attachment 2**, NGB IMT 3631, *Air National Guard Telecommuting Supervisor and Telecommuter Checklist* and **Attachment 3**).

3.2.3. Ensuring that project details (e.g., scope of work, deliverables, time schedules, etc.) are mutually agreed upon before beginning work.

3.2.4. Quality control of the telecommuter's completed product.

3.2.5. Maintaining the original approved work agreement with a copy to the telecommuter.

3.3. The commander is responsible for approving the use of Government owned equipment and supplies for use by the telecommuter. The decision to use appropriated funds to pay for equipment, services or supplies for the purposes of telecommuting rests solely with the commander.

4. Compensation.

4.1. Telecommuters will be compensated in accordance with their duty status. All telecommuters must comply with appropriate pay status regulations.

4.2. The approval authority will not authorize travel or per diem for telecommuting.

4.3. The approval authority may authorize the performance of duties on an incrementally accrued schedule for telecommuters in a military status (NGB IMT 3630, *Telecommuting Duty Form*).

4.4. Incidental expenses incurred by members may be reimbursed in accordance with current financial management policy governing claiming reimbursement from the government. Approval is not guaranteed and should be obtained prior to incurring the expense.

5. Safety. Telecommuters are responsible for ensuring that alternate work locations are safe environments. Telecommuters will report any injuries while telecommuting to their supervisor as soon as possible. The supervisor will follow line of duty reporting procedures for accidents or injuries.

6. General Obligations.

6.1. Telecommuters are subject to applicable military laws, regulations and instructions.

6.2. Telecommuters are responsible for providing telecommuting equipment requirements to the supervisor.

6.3. Telecommuters should obtain the approving authority's concurrence before performing telecommuting duties that exceed the terms or hours listed in the work agreement.

6.4. The approval authority, supervisor or telecommuter may terminate participation in telecommuting at any time.

6.5. Telecommuters will not use telecommuting for upgrade training or Professional Military Education training purposes.

6.6. Telecommuters must provide adequate and timely access to their telecommuting location for troubleshooting, equipment installation, inventory, modification, etc., if needed and to ensure telecommunications guidelines are being followed.

7. Agreements. The telecommuter, supervisor and approval authority must sign a work agreement (**Attachment 2**), Telecommuter checklist (NGB IMT 3631), and commander's authorization (**Attachment 3**), before starting the telecommuting project.

8. Miscellaneous.

8.1. Personnel will be entitled to the same protections and indemnification under the Federal Tort Claims Act as would be available if the services provided herein were provided at the unit during a Unit Training Assembly (UTA) or during scheduled active duty.

8.2. Wear of the uniform during performance of duty set forth in this instruction is not required.

8.3. Personnel falsely certifying documents under this instruction are subject to punishment and/or administrative action.

Section B—Equipment

9. Government Equipment.

9.1. Subject to prescribed rules and limitations, a commander may place government-owned computers, computer software, and telecommunications equipment (hereafter referred to as equipment) in alternative work locations.

9.2. The commander retains ownership and control of all hardware, software and data associated with, or generated by, government-owned systems. The commander must account for equipment on a hand receipt (AF IMT 1297, *Temporary Issue Receipt*) and inventory all equipment annually. The commander must notify the Equipment Control Officer (ECO) of the relocation of the equipment.

9.3. Government equipment is FOR OFFICIAL USE ONLY (FOUO). Commanders may authorize installation, repair and/or maintenance of equipment at their discretion and direction. The equipment is for authorized use by the telecommuter only.

9.4. Telecommuters must comply with all government security procedures and ensure that security measures are in place to protect equipment and data from physical and virus damage, theft, loss or access by unauthorized individuals.

9.4.1. TELECOMMUTING EQUIPMENT MAY NOT BE USED TO ACCESS OR VIEW CLASSIFIED MATERIAL.

9.4.2. ANG APPROVED ANTI-VIRUS SOFTWARE (WITH THE LATEST SIGNATURE FILE) WILL BE USED AND ACTIVE WHEN TELECOMMUTING.

9.5. Before telecommuters install any hardware or software on a government system, they must have the permission of the Designated Approval Authority (DAA). Telecommuters must ensure that software use conforms to copyright law and any contractual agreements.

9.6. Report of Survey procedures must be followed if government equipment is damaged, lost or stolen.

9.7. Government information must be protected from modification, destruction or inappropriate release.

9.8. If telecommuting is no longer required or appropriate, the telecommuter must immediately return government-owned hardware, software, data, and cancel all telecommunication services that the government provided.

9.9. The authorizing official assumes responsibility for providing any government network or computer equipment and telecommunication services required for telecommuting. Depending on circumstances, this may include dial-in capability, VPN capability, DSN access, high-speed internet access, leased-line costs, etc. Authorizing officials are not responsible for and will not assume personal costs of telecommuting such as telecommuter's home telephone or internet services.

10. Privately Owned Equipment

Frequent telecommuting using privately owned equipment presents unacceptable risk to ANG information resources and equipment. Privately owned equipment will NOT be used for telecommuting on a regular basis; government equipment should be provided for frequent telecommuting or when full network services are required. Privately owned equipment may be used intermittently for minimal public network services (e.g., e-mail via Outlook Web Access) under exceptional circumstances provided that:

10.1. User agrees to install, service, and maintain (at their own risk and expense) any privately owned equipment or services.

10.2. The government does not incur any liability or assume any costs resulting from the misuse, loss, theft or destruction (to include computer viruses) of privately-owned equipment, resources or data.

10.3. Use of DoD provided anti-virus software is required unless user already has current and updated commercial anti-virus software in place.

10.4. The user stores all government data on appropriately marked removable media.

10.5. Government information is protected from modification, destruction, misuse or inappropriate release. Users must control access to systems in use until appropriately cleared per Paragraph **10.6.**

10.6. User must remove sensitive residual government information from privately owned systems using an approved data removal method when the session is terminated. Sensitive information includes Privacy Act and For Official Use Only information, but may also include any other information deemed mission related.

10.7. User will only access network resources through approved gateway protocols and methods such as Outlook Web Access in accordance with ANG/C4 Remote Network Access Policy. NOTE: Direct connections to the network by privately owned equipment are prohibited.

10.8. The DAA approves of the access by non-government equipment. DAAs allowing use of personal equipment must ensure that procedures are in place to recover from information mishandling incidents and to ensure removal of residual government information.

10.9. User must provide adequate and timely access to privately owned equipment for troubleshooting, installation, inventory, modification, etc., in the event an information handling incident is encountered and to ensure guidelines are being followed.

10.10. Telecommuters may not "auto-forward" e-mails from government to non-government accounts as e-mail containing sensitive information may not transit public networks without appropriate encryption. E-mail and attachments may be manually forwarded after review if no sensitive information is included. This may also prevent inadvertent transit of classified information in the event such an incident occurs on the unclassified network. Telecommuters may establish an auto-reply rule to provide those wishing to contact them with alternate contact information.

Section C—Accountability

11. Documentation.

11.1. The approval authority will sign all required agreements before the telecommuter starts the telecommuting project.

11.2. The telecommuter should submit pay documentation in a timely manner. The approval authority indicates agreement by signing the appropriate pay documents (e.g., NGB 105S, *Authorization for Individual Inactive Duty Training*, etc.) annotating telecommuting status.

12. Information Management Tools (IMTs) Prescribed : NGB IMT 3630, *Telecommuting Duty Form*, and NGB IMT 3631, *Air National Guard Telecommuting Supervisor and Telecommuter Checklist*.

13. Adopted IMTs and Forms : NGB 105S, *Authorization for Individual Inactive Duty Training* and AF IMT 1297, *Temporary Issue Receipt.*

DANIEL JAMES III, Lieutenant General, USAF
Director, Air National Guard

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD 7950.1, *Automated Data Processing Resources Management*

DoD 7000.14-R, *DoD Information Security Program*

DoD 7000.14-R, Vol 8, *Civilian Pay Policy and Procedures*

DoD 7950.1-M, *Defense Automation Resource Management Manual*

AFPD 10-6, *Mission Needs and Operational Requirements Use Agreements*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *C4 Systems Security*

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance, and Training*

AFI 23-111, *Management of Government Property in Possession of the Air Force*

AFI 31-101, Vol. 1, *The Air Force Physical Security Program*

AFI 31-209, *The Air Force Resource Protection Program*

AFI 33-111, *Telephone Systems Management*

AFI 33-112, *Computer Systems Management*

AFI 33-114, *Software Management*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information via the Internet*

AFI 37-132, *Air Force Privacy Act Program*

AFMAN 23-110, Vol. 2, *USAF Supply Manua*l, Part 13, Charters 4 and 8

ANGI 36-2001, *Management of Training and Operational Support within the Air National Guard*

ANGI 65-101*, Air National Guard (ANG) Workday Accounting and Reporting Procedures*

Abbreviations and Acronyms

ANG—Air National Guard

ANGI—Air National Guard Instruction

ANG/C4—Air National Guard/Command, Control, Communications and Computers

AFPD—Air Force Policy Directive

DAA—Designated Approval Authority

DoD—Department of Defense

DSN—Defense Switch Network

ECO—Equipment Control Officer

IMT—Information Management Tools

USC—United States Code

UTA—Unit Training Assembly

VPN—Virtual Private Network

Attachment 2

AIR NATIONAL GUARD TELECOMMUTING WORK AGREEMENT

The following constitutes an agreement between:

_____ And _____ agree to

Supervisor/Approval Authority Telecommuter

the terms and conditions of the telecommuting program. The supervisor and telecommuter agree:

Telecommuting schedule is: _____ Fixed _____As needed.

A2.1. Telecommuter agrees to adhere to the applicable pamphlet, guidelines, policies, and procedures of the telecommuting program. Telecommuter recognizes that the telecommuting arrangement is not a right but a complementary tool the ANG may use to accomplish work.

A2.2. The telecommuter will meet with the approval authority/supervisor to develop and/or amend performance agreements for work performed away from the official duty station. The telecommuter will complete all assigned work according to work procedures mutually agreed upon by the telecommuter and the approval authority/supervisor in the agreement.

A2.3. Participation in telecommuting does not change the telecommuter's official duty work location.

A2.4. Where applicable, the telecommuter agrees to document and submit to the supervisor/approval authority for endorsement, any changes in the work agreement.

A2.5. The telecommuter must ensure that a safe and healthy work environment exists. If required by the supervisor/approval authority, the telecommuter agrees to sign a self-certification checklist that proclaims the alternative work site is free of work related safety and health hazards.

The alternate worksite is: _____

A2.6. Any data, document or work product developed in telecommuter's telecommuting is the sole property of the United States Government.

A2.7. During telecommuting the supervisor/approval authority may check progress via telephone calls, electronic mail or other available means.

A2.8. The telecommuter agrees not to conduct personal business while in official duty status at the telecommuting workplace (e.g., caring for dependents, making home repairs, etc.).

A2.9. The telecommuter acknowledges that while telecommuting, he/she is subject to the applicable laws, regulations and instructions during the duty hours specified relative to the duty status.

A2.10. Equipment.

A2.10.1. The Government retains ownership and control of all hardware, software, and data associated with government-owned systems.

A2.10.2. Government equipment is FOR OFFICIAL USE ONLY. Installation, repair, and maintenance are at the sole discretion and direction of the issuing organization.

A2.10.3. The telecommuter agrees to protect any government-owned equipment, to prevent the use by others, and to use the equipment only for official purposes.

A2.10.4. The telecommuter must have DAA approval before installing any hardware or software on government systems.

A2.10.5. The telecommuter agrees to install, service and maintain any privately owned equipment at the telecommuter's sole risk and responsibility. NOTE: Regular telecommuters accessing full network resources must use government furnished equipment.

A2.10.6. The government does not incur any cost or liability resulting from the use, misuse, loss, theft or destruction of privately owned computer equipment or resources. NOTE: Regular telecommuters accessing full network resources must use government furnished equipment.

A2.10.7. The telecommuter must comply with DoD, AF and ANG security procedures and ensure that security measures are in place to protect the equipment from damage, theft or access by unauthorized individuals.

A2.10.8. Access to sensitive documents, data, records, etc. on government equipment must be consistent with all DoD, AF and ANG directives and instructions. Privately owned equipment may not be used to access or view classified information. Users must remove any sensitive government information (e.g., Privacy Act, FOUO) from privately owned systems using an approved data removal method when the session is terminated.

A2.10.9. The telecommuter is responsible for providing security against loss due to malicious logic, physical or virus loss, theft, or damage. Anti-virus software is available for both government and privately owned computers.

A2.10.10. Telecommuters must provide adequate and timely access to their equipment for troubleshooting, installation, inventory, modification, etc., in the event an information handling incident is encountered and to ensure telecommuting guidelines are being followed.

A2.10.11. Telecommuters will only access network resources through approved gateway protocols and methods in accordance with ANG/C4 Remote Network Access Policy. Remote access guidelines apply to both government and privately owned equipment. NOTE: Direct connections to the network by privately owned equipment are prohibited.

A2.11. If telecommuting is no longer required or appropriate, the telecommuter must immediately return government-owned hardware, software, data and cancel all telecommunication services that the government provided.

A2.11.1. Specific telecommuting project details:

A2.11.2. Scope of work (Description of project).

A2.11.3. Projected deliverables:

A2.11.4. Estimated amount of time to complete the project:

A2.11.5. Projected start and end dates:

A2.11.6. Type of duty:

A2.11.7. Number of estimated days/periods of duty (orders required for active duty):

A2.11.8. Individual's resource requirements:

A2.11.9. Progress report requirements:

A2.11.10. Additional remarks:

_____ _____

Telecommuter Signature Date

_____ _____

Supervisors Signature Date

_____ _____

Approval Authority Signature Date

Attachment 3

COMMANDER'S AUTHORIZATION FOR OFF BASE DUTY

A3.1. You are hereby authorized and directed to perform duty under Title 32 of the United States Code at your home, civilian office and such other locations as may be reasonably convenient and most efficient in accomplishing tasks assigned to you from time to time. This authorization is given pursuant to this instruction, ANGI 36-8001, Air National Guard Traditional Guard Member Telecommuting Policy; and in accepting this authorization, you agree and understand that you are subject to the rules and constraints of this instruction. The telecommuter will be performing duty off base pursuant to the ANG Telecommuting Work Agreement and is subject to applicable ANG, Air Force and DoD instructions while telecommuting.

Figure A3.1. Sample Letter

Memorandum for _____ _____
(Authorized Member) Date

FROM: _____
(Commander)

SUBJECT: Authorization for Performance of Off Base Duty

A3.2. You will track and account for time devoted to such military duties in sufficient detail which shall be reported to me for approval under this instruction as set forth in this instruction.

A3.3. If you complete work as outlined in the agreement, I will approve your submission and authorize pay and points for the work accomplished consistent with this instruction.

A3.4. This authorization is revocable by me at any time with or without prior notice.

_____
(Signature Block)